A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2001-0210-4C

OFFICE OF THE STATE AUDITOR'S
REPORT ON INFORMATION TECHNOLOGY CONTROLS
AND THE BILLING AND RECEIVABLE SYSTEM
AT THE UNIVERSITY OF MASSACHUSETTS-DARTMOUTH

July 1, 2000 through June 29, 2001

OFFICIAL AUDIT REPORT
OCTOBER 6, 2001

2001-0210-4C

TABLE OF CONTENTS

INTRODUCTION

The Commonwealth's enactment of Chapter 146 of the Massachusetts Acts and Resolves of 1991 called for restructuring and incorporating five public institutions of higher education within the University of Massachusetts system. The former Southeastern Massachusetts University was renamed the University of Massachusetts-Dartmouth (UMD) on September 1, 1992 and was designated to be one of five campuses within the University of Massachusetts system. The UMD is overseen by the Board of Trustees for the five-campus University of Massachusetts system.

The University of Massachusetts-Dartmouth offers undergraduate and graduate degree programs in arts and sciences, business and industry, engineering, nursing, and visual and performing arts. All the University's colleges are located on a 710-acre campus. At the time of our audit, UMD had an enrollment of 6,058 day students and 1,188 continuing-education students.

UMD is heavily reliant on its information technology resources to assist in carrying out its mission. At UMD, information technology (IT) functions and services are administered through Computing and Information Technology Services (CITS) which includes: computing support, cluster/classroom operations, information systems, website development and maintenance, microcomputer maintenance and repair, networking systems, IT operations and access security. The backbone of University of Massachusetts Dartmouth campus' Ethernet network (UMDNet) provides access to campus computing activities that include e-mail, the library system, the campus web site, distance learning, and access to the Internet. UMD operates a Compaq Alpha computer cluster with an open VMS operating system to support administrative systems, programming, research, and electronic mail.

The physical UMDNet is distributed over multi-mode fiber optic cable connected through wiring closets located throughout the campus. Outside of the main campus, the network extends to include the student housing network, referred to as ResNet, which has the capability of supporting 3,000 student connections. In addition, as a hub to the Internet, the campus connects the following five regional and community colleges: Bridgewater State College, Bristol Community College, Cape Cod Community College, Massachusetts Maritime Academy, and Southern New England School of Law. Moreover, the campus maintains a connection for the Cape Libraries Automated Material Sharing, the Commonwealth's Human Resources/Compensation Management System (HR/CMS), and the Massachusetts Management

Accounting and Reporting System (MMARS). UMD's satellite campus located in New Bedford, which includes the School of Marine Science and the Star Store, and the Advanced Technology Center in Fall River are connected via leased T-1 telephone lines and microwave dish communication for voice, data and video. Remote access to the UMD campus and to the Internet is accomplished by an external Internet service provider and secured with a virtual private network gateway that offers encryption of remote transactions.

A router that is connected to a LAN via an Ethernet link facilitates off-campus connectivity and the five-campus network is connected via a DS-3 link to the Massachusetts Information Technology Initiative (MITI) within the Prudential building facility in Boston. The MITI is a 120-mile fiber optic broadband network that links the University of Massachusetts's five campuses with the Commonwealth's 24 state colleges and community colleges and more than 150 libraries.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

Our audit, which was conducted from February 1, 2001 through June 29, 2001, consisted of an examination of selected controls related to the IT processing environment and the Billing and Receivable System at the University of Massachusetts Dartmouth (UMD) covering the period of July 1, 2000 through June 29, 2001. Our audit scope included an examination of IT-related controls pertaining to organization and management, physical security and environmental protection of IT equipment in the data center and selected sites housing IT resources throughout the University including computer labs and wiring closets, disaster recovery and business continuity planning, and on-site and off-site storage of backup magnetic media. We also reviewed controls for fixed-asset inventory for IT resources, and system access security for functions and systems residing on the VAX and Alpha clusters. In addition, we reviewed selected areas in the Billing and Receivable System (BRS), which is a sub-system of the Student Information System (SIS).

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for selected functions of the IT processing environment and the Billing and Receivable System. We sought to determine whether the University's IT-related internal control environment, including policies, procedures, practices, and organizational structure provided reasonable assurance that control objectives would be achieved to support business functions. We sought to determine whether adequate physical security and environmental protection controls were in place over IT operations including computer labs and wiring closets. We also sought to determine whether adequate controls were in place to prevent and detect unauthorized system access to the data files and software residing on the VAX and Alpha clusters and certain microcomputer systems. Regarding the availability of systems, we sought to determine whether adequate business continuity plans were in effect to provide reasonable assurance that mission-critical and essential systems could be regained within an acceptable period of time should a disaster render processing inoperable. Moreover, we determined whether adequate on-site and off-site storage was being provided for critical backup copies of magnetic computer media. With regard to inventory controls over fixed assets, we evaluated whether fixed assets were safeguarded from unauthorized use and theft, whether these assets were accurately reflected in the

fixed-asset inventory and accounting records, and whether an annual physical inventory was conducted.

In addition, we sought to determine whether the data in the Billing and Receivable System (BRS) application, a sub-system of the Student Information System (SIS), remained complete, accurate, and valid during input, update, and storage.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work, which included obtaining and recording an understanding of relevant operations, performing a preliminary review and evaluation of IT-related internal controls, and interviewing senior management to discuss the University's control environment.

To accomplish a preliminary review of the adequacy of general controls over IT-related operations and resources, we obtained an understanding of IT operations at the University. We conducted site visits to the UMD data center and selected sites throughout the campus housing microcomputers. We performed a risk analysis of selected IT operations and selected application areas. To assess the adequacy of selected internal controls regarding IT and selected application operations, we interviewed management and staff, observed operations, and performed selected audit tests.

Regarding our review of organization and management, we interviewed senior management, reviewed and analyzed documentation, and assessed other IT-related internal controls. To determine whether IT-related assets and other assets related to IT operations were adequately safeguarded from damage or loss, we reviewed physical security and environmental protection over computer operations through observation and interviews with UMD staff.

To test whether physical security and environmental protection controls were in place and in effect within the UMD's wiring closets, we selected 10% of the wiring closets on campus to document whether adequate physical and environmental controls were in place. We inspected the selected closets and interviewed management regarding physical security and environmental protection of the wiring closets.

For our examination of the computer labs, we interviewed senior management, reviewed policies and procedures, and completed questionnaires. We selected 25% of the labs to observe whether adequate physical and environmental controls were in place and in effect. We also reviewed the contract agreement with Charlton College of Business and CITS for the appropriateness of the terms and conditions.

Our tests of system access security included a review of access privileges of UMD's employees authorized to access the mainframe, LAN, and microcomputer systems. To determine whether access security was being properly maintained through the management of user IDs and passwords, we interviewed the security administrator and assessed the level of access security being provided. To determine whether access privileges existing on the system were authorized, we reviewed procedures for granting system access. We determined whether procedures were in place to ensure that the security administrator was promptly and properly notified of a change in personnel status (e.g., employment termination, job transfer, or leave of absence) so that the user ID and password could be promptly deactivated from the system or the access privileges be appropriately modified. We completed a 100% review of the user access list to determine whether 1,123 active user accounts were assigned to authorized users employed by UMD.

To assess the adequacy of disaster recovery and business continuity planning, we determined whether any formal planning had been performed to resume computer operations in a timely manner should automated systems be damaged, destroyed, or rendered inoperable. To evaluate the adequacy of controls to protect mainframe, LAN, and microcomputer-based data files and software, we interviewed management at UMD and reviewed the current business continuity plan. Further, we interviewed management and staff and assessed the frequency of transfer of newly-generated copies of backup media to on-site and off-site storage, and assessed physical security and environmental protection for on-site and off-site computer media storage.

With regard to our review of fixed assets, we evaluated whether fixed assets were properly accounted for and controlled. Initially, we reviewed the University of Massachusetts-Dartmouth's documented inventory control and management procedures, reviewed the record layout for the appropriateness of required information, and obtained a sample of the inventory record for testing and to assess the comprehensiveness of the included data. We then assessed the adequacy of inventory controls by assessing the integrity of the inventory record, determining whether equipment was properly tagged with UMD identification numbers and determining whether annual inventory reconciliations were performed. To determine whether inventory records were current, accurate, complete, and valid, we selected a judgmental sample of items from the master inventory list and traced them from the inventory list to their physical locations. We also verified whether a current record was maintained for software products for microcomputer and LAN-based software.

To evaluate the Billing and Receivable System (BRS), we interviewed senior management from the Bursar's Office and the Student Enrollment Center. We also reviewed relevant policies and procedures to obtain and record an understanding of the process for collecting, recording and

depositing cash receipts. To evaluate controls for timely deposits of cash receipts, we reviewed the University's policies and procedures as maintained through the Bursar's office. We compared a sample of billing and receivable records produced by the automated system to the actual student records by randomly selecting two days of cash receipts in the University's Bursar Office.

We reviewed cashier checkout reports, daily batches, bank deposit slips, armored car receipts, credit card receipts, cash receipt entry logs, daily on-line transcript reports, weekly reports, bank reconciliations and student account history files. We traced the transactions from selected days of the cash collection process to the student account history files by verifying the source documents to the reports that were generated by the automated system. Additionally, we traced the cash receipts to the bank deposit slips and the bank reconciliation reports and the credit card receipts to the batch reports and bank records.

Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and industry auditing practices.

AUDIT SUMMARY

Based on our audit at the University of Massachusetts-Dartmouth, we found that there was reasonable assurance that IT-related control objectives would be met by internal controls in place with respect to IT organization and management, physical security, environmental protection, business continuity planning, on-site and off-site storage of backup computer media, and logical access security for the VAX and Alpha clusters and associated local area networks and related workstations. With respect to inventory controls, our review of the policies and procedures regarding fixed-asset inventory indicated that, although the policies for conducting inventory were adequate, they were not being followed. With respect to the integrated Student Information System, our tests of data management and data integrity for the Billing and Receivable System (BRS) indicated that for the data selected, controls were in place to provide reasonable assurance that the data would remain current, accurate, complete, and valid during data input, update, and storage. With respect to controls related to timely deposits of cash receipts, we found that policies, while requiring timely deposits, did not indicate a specific time frame, and that monitoring procedures for timely deposits were not formalized. In addition, our audit determined that controls needed to be strengthened to provide greater assurance that deposits would be made on a daily basis as required by the Office of the State Comptroller.

Our review of the UMD's organization and management over IT-related activities disclosed that adequate organizational controls were in place and that documented policies and procedures existed and were appropriate. Further, regarding IT-related organization and management, we found that there were sufficient controls in place with respect to reporting lines, segregation of duties, span of control, and oversight. Overall, we also found that organizational controls had been strengthened by implementing centralized control and a single point of accountability for IT services.

We determined that adequate physical security controls were in place to safeguard IT-related resources in the data center. However, we found that physical security controls over the hub networking center in the UMD's textile building needed to be strengthened. In addition, our tests of environmental controls over the hub networking area in the textile building indicated that controls needed to be strengthened to reduce the exposure of IT equipment to excessive dust from machinery located in the area.

We found that environmental protection controls were in place in the data center for temperature and humidity levels, smoke detection and fire suppression, and general housekeeping. UMD maintains two uninterruptible power supply (UPS) units in the data center, as well as additional UPS units in the wiring closets located throughout the campus to help ensure continued power for a short time for critical IT-related resources. The UPS units provide protection against power spikes and brownouts and allow the equipment to be powered down in a logical sequence without potential damage to data or system integrity.

Our tests of selected computer labs indicated that although there were adequate physical security and environmental protection controls in place in the labs that are under the direct control of CITS, one of the selected labs, which had a partnership with the Charlton College of Business, needed stronger physical security controls. Our tests revealed that the alarm system was not engaged, the door was often left ajar, and the room was unattended, thereby exposing the IT equipment to the possible threat of loss or misuse.

We found that appropriate procedures were in effect for making backup copies of magnetic media and for storing the backups on-site as well as at a contracted off-site location. We further determined that the storage facility housing on-site backup copies of computer-related media was adequately safeguarded and environmentally protected. In addition, CITS had developed a comprehensive business continuity plan that outlined a sound strategy for maintaining system availability in the event of a major disaster or disruption of IT operations. Furthermore, the University's documented procedures, if followed, provided reasonable assurance that IT operations could be recovered should IT equipment become damaged, inoperable or inaccessible. Although additional business continuity testing is recommended, we noted that the plan had been tested partially on June 10, 2001 by a planned electrical shutdown. This particular test involved the staff having to perform specific duties in order to bring the systems down logically to simulate a real disaster and then reestablish system operations. We recommend that the UMD continue to test its disaster recovery and business continuity plan on a regular basis in order to assess its viability. We also recommend that a process be established for routinely updating the plan based on changes to the technology, business processes, staffing, or threats and vulnerabilities to the IT processing environment.

Based on our review of system access security, UMD's policies and procedures appear to provide reasonable assurance that only authorized users have access to the applications and workstations connected to the local area network and wide area network. We found that policies regarding controls over the administration of user IDs and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified in a timely

manner should individuals having access terminate employment or incur a change in job requirements. Our review of the access security list indicated that, as of the date of our test, all user accounts were assigned to authorized UMD employees.

Our review of fixed-asset inventory indicated that controls needed to be strengthened to provide reasonable assurance that fixed assets are safeguarded and properly accounted for. We found that a physical inventory of fixed assets had not been conducted within the last five years, which could result in inventory records being inaccurate and incomplete. Our review of fixed-asset inventory controls also indicated that although UMD maintained an inventory list tracking appropriate information, we believe that controls could be strengthened to assure proper tracking of the items on the inventory list. The University did not have adequate control procedures to monitor changing location of inventory items, specifically hardware items. For example, we found certain information on the inventory list needed to be updated to reflect the current location of certain computer equipment.

At the time of our audit, we found that certain IT resources were not at the identified location and that the tag numbers did not always match the inventory listing. Based on a judgmental audit test of the UMD's inventory record of IT resources, we determined that 80% of the tested assets were in the location indicated on the master inventory listing, while 20% were not. Although the items could not be located by UMD to verify the asset's inventory status, we acknowledge that this does not necessarily imply that the items were lost or stolen, but more likely that they had been moved without proper authorization, notification, or change to the inventory record. Our audit test did not include IT resources purchased over the audit period.

Although our tests performed on the Billing and Receivable System (BRS) indicated that controls over data integrity were adequate, controls over timely deposit of cash receipts needed to be strengthened. Specifically, our tests of BRS, a sub-system of the Student Information System (SIS), indicated that there were adequate controls in place to ensure that cash receipts were accurately tracked and accounted for during the receivable collection process, not only on the University's summary reports, but also on the students' individual account records. However, our review disclosed that although policies and procedures exist for timely deposits of cash receipts, monitoring activities needed to be strengthened to ensure that deposits of cash receipts are made on a daily basis from all areas of the university. We found that deposits were not always done on a daily basis. Specifically, our limited judgmental tests found that $89,324 in receipts was not deposited for 13 days.

AUDIT RESULTS

1. Deposit of Cash Receipts

Our review of the data management and data integrity for the Billing and Receivable System (BRS), a sub-system of the Student Information System (SIS), indicated that for the data selected, controls were in place to provide reasonable assurance that the data would remain complete, accurate, and valid during data input, update, and storage. As part of the review of BRS, we evaluated the policies and procedures the University had in place to assure daily deposits of cash receipts. With respect to controls related to timely deposits of cash receipts, we found that policies, while requiring timely deposits, did not indicate a specific time frame and that monitoring procedures for timely deposits were not formalized. We then tested selected cash receipts from the time they were received to the time they were deposited in the bank. Our test included nine batches that totaled $305,778 in cash receipts and five credit card batches that totaled $14,257. The results of our test revealed that controls needed to be strengthened in this area since two batches of cash receipts that totaled $89,324 were found not to be deposited for thirteen days from the time the paper work, including the recording of cash receipts and batched totals being prepared by the accounting department, had been completed until the time the deposit was picked up by the courier service to be delivered to the bank.

Massachusetts General Laws (MGL), Chapter 30, subsection 27, requires that "all fees and other monies received on account of the Commonwealth shall be paid daily into the treasury thereof." Furthermore, the Office of the State Comptroller's Internal Control Guide, promulgated under Chapter 647 of the Acts of 1989, requires that all receipts be deposited with the appropriate depository within one business day of receipt for sweep by the Office of the State Treasurer. Although these funds may not be directly forwarded to the State Treasurer, the law with respect to timeliness still applies. In addition, prudent business practices indicate that monies collected should be deposited in a timely manner to assure proper control over the cash receipts. The UMD's Bursar's Office has written procedures for the different types of transactions that are handled at both the Student Enrollment Center and the accounting department, including how to accept and record deposits; however, there was no reference to the required frequency of deposits. Although controls were adequate over the recording of checks received and procedures existed to ensure monthly reconciliation of batch totals to cash received and deposited, delays in depositing checks may lead to the risk of the loss or theft of checks, or lost interest revenue due the Commonwealth.

According to UMD management, the Bursar's Office was understaffed which had resulted in the staff not always being able to prepare the deposits on a daily basis. Because the Bursar's Office processes and deposits approximately $30 million yearly, it is necessary to monitor cash receipt processing to help ensure timely deposits of cash receipts.

Recommendation:

We recommend that the University ensure the timeliness of making deposits of received cash and checks by adapting their policies to comply with MGL, Chapter 30, subsection 27 as well as the Comptroller's guidelines that indicate deposits should be done on a daily basis. Unless the University has applied for and received an exemption permitted by MGL, Chapter 30, subsection 27, we further recommend that efforts be made to improve controls to ensure that checks are deposited on a daily basis by reassigning staff to monitor this activity. In addition, as a means of monitoring processing time of cash receipts to the deposit of these receipts, UMD's Bursar's Office should instruct the accounting department to time stamp all cash receipts as soon as they are received.

Auditee's Response:

> *As a result of the IT audit findings, the Bursar's Office staff is time and date stamping all receipts submitted by other areas on campus. This will help to support the timeliness in which funds are deposited.*
>
> *The staff member responsible for deposit preparation has been instructed to notify the Bursar when the volume of receipts will prohibit timely deposits. The Bursar then will utilize any resources (if available) to assist with this process.*

Auditor's Reply:

We agree with these actions for recording the date of cash receipts and implementing procedures for ensuring timely deposit of cash receipts.

2. Physical Security and Environmental Protection

a. Physical Security Controls:

Although we found that physical security over the data center and selected sites housing microcomputers within the University was adequate, we found that controls needed to be strengthened in the computer labs that are partnered with the Charlton College of Business (CCB) and the hub networking center that is located in the Textile Building.

Our audit of the 16 computer labs located throughout the campus included interviews with management, review of policies and procedures, and observation of four of the labs for adherence to physical security controls. We observed that the door to one of the labs (Room II-210) was unlocked, unmonitored, and the alarm was not engaged. In addition, both the connecting door to room 209, as well as the primary entrance door to room 209, were also left ajar. This lab is operated by the CCB for instructional purposes. For those hours in which CCB does not hold classes, student access hours are in effect.

CITS and CCB had entered into a written contract, signed on April 11, 2001, which states that "CITS accepts responsibility for physical security of II-210 and the equipment when it is staffed/utilized by CITS." CCB accepts responsibility for physical security of II-210 and equipment when it is staffed/utilized by CCB. At the time of our audit, we were advised that CITS did not have responsibility over II- 210 because student access hours for this room ended at the conclusion of the Spring 2001 semester, and therefore, it was the responsibility of the CCB to lock the door and engage the alarm when they were finished using Room II-210. These control weaknesses were, in part, the result of a lack of monitoring of the distribution of keys for the computer labs.

Our test of physical security over the hub networking center indicated that the stackable rack, containing IT equipment, in the textile building was located out in an open area and near an unlocked door to the outside. IT general controls require that IT equipment be adequately safeguarded and maintained in a physically secure area. The lack of physical security controls increased the risk of unauthorized access, use, damage, or theft.

Recommendation:

We recommend that UMD ensures that the CCB adhere to the terms and conditions of the contractual agreement that they had entered into with CITS concerning the management and oversight of the computing lab in II-210 and ensure that CCB strengthens its controls concerning the distribution of keys to the labs. In addition, we recommend that the stackable rack in the textile building be placed in a locked cabinet so that the IT equipment will be protected from unauthorized access, use, damage or theft.

Auditee's Response:

> *As of August 2001, the Marketing Department and Faculty with offices in Group II-209 are now on notice that security is a critical issue and no door is to be left ajar. Faculty offices in Group II-209 will not be available to faculty as of the year 2003.*

The agreement of the Charlton College of Business with Computing and Information Technology Services (CITS) to have physical security over Group II-209 and Group II-210 was re-established in the summer of 2001 whereby discussions for ensuring security are ongoing. CITS now monitors key distribution and access, including re-keying locks as appropriate. Faculty requesting to use a lab must sign a security agreement with the Charlton College of Business for locking doors, etc. during the times in which CITS personnel are not present.

If security is violated by a faculty member, he/she will be given verbal notice of the violation on the first occurrence, written notice on the second occurrence and denied access to keys or the labs for a period of thirty days on the third occurrence. After a third occurrence, the faculty will only have supervised access to the lab for a period of one calendar year. The Dean of the Charlton College of Business will manage all security infractions.

Auditor's Reply:

We commend the actions taken to improve physical security concerns and recommend regular monitoring to ensure that CITS have implemented their new security procedures. We suggest that, in light of current events, that the University reassess the security of exterior doors for all campus buildings.

b. Environmental Protection:

Our review of environmental protection controls in the data center and selected sites housing microcomputers within the University indicated that controls appeared to be adequate, except for the stackable rack containing IT equipment in the Textile Building. We found that this IT equipment was located in an unprotected area near machinery that produced a high volume of dust. General control practices related to computer environments require that IT equipment be maintained in areas that are environmentally protected to ensure proper operation and the safeguarding of IT related assets. IT general control procedures also require that adequate and reasonable environmental controls exist within all IT facilities to prevent vulnerabilities that could cause interruptions to continuous IT operations. As a result of the placement of the IT equipment in the Textile Building, the potential for damage to this equipment exists. Although the University indicated limited space for this IT equipment, control procedures must be adhered to.

Recommendation:

We recommend that the stackable rack containing IT equipment be placed in an enclosed cabinet in order to protect it from the high dust factor and safeguard the University's IT equipment from other potentially damaging environmental factors.

Auditee's Response:

Although the Textile Building services relatively few devices on the campus network, it is important that those devices be connected and protected. In response to the finding of network equipment in an unprotected and environmentally unfit location, Computing and Information Technology Services (CITS) will purchase a secure rack enclosure and will place the network equipment in that secure rack. The rack will only be accessed by CITS network personnel. The equipment will be purchased this fiscal year.

Auditor's Reply:

We believe that a secure rack enclosure will provide proper environmental controls for the network equipment located in the Textile Building.

3. Fixed-asset Inventory Control

Our review of the policies and procedures regarding fixed-asset inventory indicated that, although the policies for conducting inventory were adequate, they were not being followed. We found that a physical inventory of assets had not been conducted within the last five years, which could result in inventory records being inaccurate and incomplete. UMD Inventory Control and Property Management policy states that "all equipment owned by the University which has an actual cost of $1,000 or more and a life expectancy of two years or more, said equipment shall be inventoried every two years."

Our review of fixed-asset inventory controls also indicated that although the University maintained an inventory list tracking appropriate information, we believe controls could be strengthened. For example, we found certain information on the inventory list required updating to reflect the current location of certain fixed assets. At the time of our audit, we found that certain assets were not at the specified location and that the tag numbers did not always match the inventory listing.

Our tests of UMD's inventory record, consisting of a judgmental sample of 35 hardware items out of the fixed-asset inventory which totaled of 8,717 items, revealed that 80% of the tested assets were in the location indicated on the master inventory listing, while 20% were not.

Although the items could not be located by UMD to verify the assets inventory status, we acknowledge that this does not necessarily imply that the items were lost or stolen, but more likely that they had been moved without either proper authorization or notification to the Asset Manager. These conditions indicate that procedures need to be strengthened to ensure notification to the Asset Manager when the location of equipment is changed. We did not include newly-purchased items in our audit test.

Recommendation:

We recommend that UMD enforce its policies and procedures regarding the recording of fixed asset inventory as indicated in "UMD Inventory Control and Property Management " policy by ensuring the completion of an annual physical inventory for all department locations so that the asset inventory record can be appropriately updated, verified for accuracy, and maintained on a perpetual basis. In addition, assets should not be moved without the prior approval of and notification tot he Asset Manager.

Auditee's Response:

The Property Control Office at UMass Dartmouth maintains a rolling and continuing inventory of its fixed assets. Under the current staffing of the Office, asset management is done on a part-time basis because the one position we have has remained vacant for the last several months.

A request has been made to fill the vacant position in the Property Control Office. Once the position is filled, we will be able to conduct a scheduled inventory.

It is most difficult to maintain an accurate inventory for the following reasons.

1. *Faculty and staff are relocated to different offices yearly with no notice to the Property Control.*

2. *Many of our staff use laptop computers for office and home use. This limits our ability to locate such equipment on a selective and random basis.*

At the beginning of each academic year, we will reinforce our off campus equipment policy by issuing a general notice to the UMass Dartmouth community.

Auditor's Reply:

We agree with the University's attempt to fill the property control office vacancy. We recognize the difficulties in establishing and maintaining a complete inventory record. However once a complete, accurate and verifiable inventory record is established through an annual physical count of all items and reconciliation with procurement and surplus records, maintenance of the system of inventory record would be facilitated by establishing perpetual inventory procedures. We suggest that the University consider cyclical testing and input from other sources to provide information on data fields requiring update. For example, when equipment is moved, there is an opportunity to verify certain information regarding the equipment being relocated and to check whether inventory tags remain affixed. The relocation documentation could be forwarded to those responsible for maintaining the inventory record to change the equipment location field and update any other fields that may be necessary. Furthermore, individual department heads could be instructed to initiate a count of all fixed assets assigned to their division and then forward this information into a central business office location for update to the inventory system of record. The information gathered should include all fixed assets on campus as well as assigned IT resources, such as laptops and printers, regardless of their location.